LANDTAG MECKLENBURG-VORPOMMERN **Drucksache 6/1630**
6. Wahlperiode **06.03.2013**

GESETZENTWURF

der Landesregierung

Entwurf eines Gesetzes zur Änderung des Landesverfassungsschutzgesetzes und des Sicherheits- und Ordnungsgesetzes zur Regelung der Bestandsdatenauskunft

A Problem und Ziel

Das Bundesverfassungsgericht hat am 24. Januar 2012 im Rahmen einer Verfassungsbeschwerde gegen mehrere Vorschriften im Telekommunikationsgesetz (TKG) unter anderem über die Verfassungsmäßigkeit der Regelungen zum manuellen Auskunftsverfahren in § 113 TKG entschieden (Az.: 1 BvR 1299/05). Es kommt in seiner Entscheidung zu dem Schluss, dass die Vorschrift so auszulegen ist, dass sie für Auskunftsverlangen in Bereichen, deren Regelung dem Landesrecht vorbehalten ist, spezifische Rechtsgrundlagen der Länder voraussetzt, die eine Auskunftsverpflichtung der geschäftsmäßigen Anbieter von Telekommunikationsdiensten (Diensteanbieter) eigenständig begründen. Demnach kann im TKG zwar die Befugnis und die Verpflichtung für die Diensteanbieter geregelt werden, bestimmte Telekommunikationsdaten an die berechtigten Stellen zu übermitteln. Ergänzend bedarf es aber in den jeweiligen Fachgesetzen des Bundes und der Länder qualifizierter Vorschriften, die den berechtigten Stellen erlauben, diese Daten überhaupt bei den Diensteanbietern abzufordern (sogenanntes „Doppeltürenmodell“).

Zudem gelangte das Bundesverfassungsgericht zu der Auffassung, dass § 113 Absatz 1 Satz 1 TKG nicht als Rechtsgrundlage - wie bisher in der Praxis erfolgt - für eine Zuordnung von dynamischen Internetprotokoll-Adressen (IP-Adressen) zu ihren Anschlussinhabern herangezogen werden kann, da für diese Auskunft auf Verkehrsdaten zurückgegriffen werden muss und die Vorschrift hierzu erkennbar nicht ermächtigt.

Darüber hinaus stellte das Gericht fest, dass § 113 Absatz 1 Satz 2 TKG nicht mit dem Recht auf informationelle Selbstbestimmung vereinbar ist, da die Vorschrift die Auskunft über Zugangssicherungscodes (wie Passwörter, PIN oder PUK) nicht an die Bedingung knüpft, dass eine Auskunft über Sicherungscodes nur dann verlangt werden darf, wenn auch die rechtlichen Voraussetzungen für deren Nutzung erfüllt sind.

Aufgrund des sich aus dieser Entscheidung ergebenden, gesetzgeberischen Handlungsbedarfs - nämlich der Schaffung normenklarer Regelungen für die Beauskunftung von Bestandsdaten im Bundes- und auch Landesfachrecht - und angesichts der Bedeutung solcher Datenauskünfte für die Aufklärung von Gefahren und Straftaten hat das Bundesverfassungsgericht eine Übergangsregelung getroffen. Es hat die Anwendung des bestehenden § 113 TKG - teilweise unter zusätzlichen Maßgaben - längstens bis zum 30. Juni 2013 zugelassen.
Der Bundesgesetzgeber hat seinen Gesetzentwurf zur Änderung des Telekommunikationsgesetzes und zur Neuregelung der Bestandsdatenauskunft bereits vorgelegt (Bundestagsdrucksache 17/12034). Er sieht eine Neufassung des § 113 TKG vor. Auskünfte über die in § 113 Absatz 1 aufgeführten Telekommunikationsdaten sollen durch die Diensteanbieter an die berechtigten Stellen zukünftig nur noch dann erteilt werden dürfen, wenn die jeweils berechtigte Stelle eine gesetzliche Bestimmung vorweisen kann, die ihr eine Beauskunftung dieser Daten bei den Diensteanbietern ausdrücklich erlaubt. Der Gesetzentwurf beschränkt sich auf die zur Umsetzung der nach der Bundesverfassungsgerichtsentscheidung notwendigen und durch den Bund möglichen Änderungen, um den Status quo aus Sicht des Bundes hinsichtlich der Gewährung von Bestandsdatenauskünften zu wahren. Er enthält jedoch keine Befugnisse zur Sicherung des Status quo für die Landesbehörden. Die Schaffung dieser fällt in die Gesetzgebungszuständigkeit der Länder.

Damit die Möglichkeit der Abfrage von Bestandsdaten nach dem neugefassten § 113 TKG der Landespolizei und der Verfassungsschutzbehörde des Landes Mecklenburg-Vorpommern auch nach Auslaufen der vom Bundesverfassungsgericht gesetzten Übergangsfrist weiter zur Verfügung steht, besteht landesgesetzgeberischer Handlungsbedarf.

B Lösung

Unter Beachtung der bundesverfassungsrechtlichen Vorgaben und des neugefassten § 113 TKG sind klare Bestimmungen im Landesrecht zu schaffen, die die Voraussetzungen für das Erlangen von Datenauskünften nach § 113 TKG von den Diensteanbietern festlegen. Diese spezifischen Befugnisse werden für die Landespolizei im Sicherheits- und Ordnungsgesetz und für die Verfassungsschutzbehörde im Landesverfassungsschutzgesetz aufgenommen. Dabei beschränken sich die mit diesem Gesetz jeweils vorgesehenen Änderungen auf die Sicherung des Status quo bei der Erlangung von Bestandsdatenauskünften nach Wegfall der vom Bundesverfassungsgericht getroffenen Übergangsregelung. Es werden keine neuen Datenerhebungsbefugnisse geschaffen. Vielmehr werden die derzeit auf Grundlage des Bundesrechts abgeforderten Datenauskünfte (bisheriger § 113 TKG) nun zukünftig unter Bezugnahme auf landesrechtliche Normen, die den verfassungsrechtlichen Vorgaben entsprechen, verlangt.

C Alternativen

Keine.

D Notwendigkeit

Die Notwendigkeit dieser Regelung wurde gemäß § 3 Absatz 1 Satz 1 GGO II geprüft. Die vorgeschlagene Aufnahme von Befugnissen zum Erlangen bestimmter Telekommunikationsdaten im manuellen Auskunftsverfahren im Landesverfassungsschutzgesetz und im Sicherheits- und Ordnungsgesetz ist aufgrund der vorgenannten Entscheidung des Bundesverfassungsgerichts erforderlich, um den derzeitigen Status quo beim Erlangen von Bestandsdatenauskünften für die Landespolizei und die Verfassungsschutzbehörde des Landes Mecklenburg-Vorpommern auch nach Auslaufen der vom Bundesverfassungsgericht gesetzten Übergangsfrist weiterhin beizubehalten.

Erhalten die Polizei oder die Verfassungsschutzbehörde Datenauskünfte im manuellen Auskunftsverfahren nach § 113 TKG, wird damit in bestimmte Grundrechte der hiervon betroffenen Personen eingegriffen. Dies setzt nach dem Grundsatz vom Vorbehalt des Gesetzes das Vorliegen entsprechender gesetzlicher Ermächtigungen voraus. Diesem Grundsatz wird durch die Ergänzung beziehungsweise Änderung sowohl des Landesverfassungsschutzgesetzes als auch des Sicherheits- und Ordnungsgesetzes Rechnung getragen.

E Finanzielle Auswirkungen auf die Haushalte des Landes und der Kommunen

1 Haushaltsausgaben ohne Vollzugsaufwand

Der Gesetzentwurf ist nach derzeitigem Kenntnisstand kostenneutral.

Der Aufwand für die Auskunftserteilung im manuellen Auskunftsverfahren wird den betroffenen Diensteanbietern - wie bisher auch - nach § 23 des Justizvergütungs- und -entschädigungsgesetzes (JVEG) entschädigt.

2 Vollzugsaufwand

Die Maßnahmen werden durch das vorhandene Personal getroffen.

F Sonstige Kosten

Für die jeweils betroffenen Diensteanbieter entsteht gegenüber der bisherigen Regelung kein zusätzlicher Erfüllungsaufwand.
Der Aufwand für die Auskunftserteilung wird den betroffenen Unternehmen nach § 23 JVEG entschädigt.

G Bürokratiekosten

Durch das Gesetz werden keine Informationspflichten für Unternehmen eingeführt.

DER MINISTERPRÄSIDENT
DES LANDES
MECKLENBURG-VORPOMMERN

Schwerin, den 6. März 2013

An die
Präsidentin des Landtages
Mecklenburg-Vorpommern
Frau Sylvia Bretschneider
Lennéstraße 1

19053 Schwerin

Betr.: Entwurf eines Gesetzes zur Änderung des Landesverfassungsschutzgesetzes und des Sicherheits- und Ordnungsgesetzes zur Regelung der Bestandsdatenauskunft

Sehr geehrte Frau Präsidentin,

als Anlage übersende ich Ihnen den von der Landesregierung am 5. März 2013 beschlossenen Entwurf des vorbezeichneten Gesetzes mit Begründung.

Ich bitte, die Beschlussfassung des Landtages herbeizuführen.

Federführend ist das Ministerium für Inneres und Sport.

Mit freundlichen Grüßen

Erwin Sellering

ENTWURF

eines Gesetzes zur Änderung des Landesverfassungsschutzgesetzes und des Sicherheits- und Ordnungsgesetzes zur Regelung der Bestandsdatenauskunft

Der Landtag hat das folgende Gesetz beschlossen:

Artikel 1
Änderung des Landesverfassungsschutzgesetzes

Das Landesverfassungsschutzgesetz vom 11. Juli 2001 (GVOBl. M-V S. 261), das zuletzt durch Artikel 2 des Gesetzes vom 28. Januar 2009 (GVOBl. M-V S. 82) geändert worden ist, wird wie folgt geändert:

1. In der Inhaltsübersicht wird nach der Angabe zu § 24a folgende Angabe eingefügt:

   „§ 24b Weitere Auskunftsverlangen“.

2. Nach § 24a wird folgender § 24b eingefügt:

„§ 24b
Weitere Auskunftsverlangen

(1) Soweit dies zur Erfüllung der Aufgaben der Verfassungsschutzbehörde erforderlich ist, darf von demjenigen, der geschäftsmäßig Telekommunikationsdienste erbringt oder daran mitwirkt, Auskunft über die nach den §§ 95 und 111 des Telekommunikationsgesetzes vom 22. Juni 2004 (BGBl. I S. 1190), das zuletzt durch Artikel 1 des Gesetzes vom … (BGBl. I S. …)[1] geändert worden ist, erhobenen Daten verlangt werden (§ 113 Absatz 1 Satz 1 des Telekommunikationsgesetzes). Bezieht sich das Auskunftsverlangen nach Satz 1 auf Daten, mittels derer der Zugriff auf Endgeräte oder auf Speichereinrichtungen, die in diesen Endgeräten oder hiervon räumlich getrennt eingesetzt werden, geschützt wird (§ 113 Absatz 1 Satz 2 des Telekommunikationsgesetzes), darf die Auskunft nur verlangt werden, wenn die gesetzlichen Voraussetzungen für die Nutzung der Daten vorliegen.

(2) Die Auskunft nach Absatz 1 darf auch anhand einer zu einem bestimmten Zeitpunkt zugewiesenen Internetprotokoll-Adresse verlangt werden (§ 113 Absatz 1 Satz 3 des Telekommunikationsgesetzes).

[1] Der Beschluss des Gesetzes (siehe Bundestagsdrucksache 17/12034) steht noch aus.

(3) Von einer Beauskunftung nach Absatz 2 ist die betroffene Person zu benachrichtigen. Die Benachrichtigung erfolgt, soweit und sobald eine Gefährdung des Zwecks der Auskunft und der Eintritt übergreifender Nachteile für das Wohl des Bundes oder eines Landes ausgeschlossen werden können. Sie unterbleibt, wenn ihr überwiegende schutzwürdige Belange Dritter oder der betroffenen Person selbst entgegenstehen. Wird die Benachrichtigung nach Satz 2 zurückgestellt oder nach Satz 3 von ihr abgesehen, sind die Gründe aktenkundig zu machen.

(4) Aufgrund eines Auskunftsverlangens nach Absatz 1 oder Absatz 2 hat derjenige, der geschäftsmäßig Telekommunikationsdienste erbringt oder daran mitwirkt, die zur Auskunftserteilung erforderlichen Daten unverzüglich, vollständig und richtig zu übermitteln.

(5) Die Verfassungsschutzbehörde hat für ihr erteilte Auskünfte eine Entschädigung zu gewähren, deren Umfang sich nach § 23 und Anlage 3 des Justizvergütungs- und -entschädigungsgesetzes vom 5. Mai 2004 (BGBl. I S. 718, 776), das zuletzt durch Artikel 13 des Gesetzes vom 5. Dezember 2012 (BGBl. I S. 2418) geändert worden ist, bemisst. Die Vorschriften über die Verjährung in § 2 Absatz 1 und Absatz 4 des Justizvergütungs- und -entschädigungsgesetzes finden entsprechend Anwendung.

(6) Das Grundrecht des Fernmeldegeheimnisses (Artikel 10 des Grundgesetzes) wird nach Maßgabe des Absatzes 2 eingeschränkt.“

Artikel 2
Änderung des Sicherheits- und Ordnungsgesetzes

Das Sicherheits- und Ordnungsgesetz in der Fassung der Bekanntmachung vom 9. Mai 2011 (GVOBl. M-V S. 246) wird wie folgt geändert:

1. In der Inhaltsübersicht wird nach der Angabe zu § 28 folgende Angabe eingefügt:

   „§ 28a Erhebung von Telekommunikationsdaten im manuellen Auskunftsverfahren“

2. Nach § 28 wird folgender § 28a eingefügt:

„§ 28a
Erhebung von Telekommunikationsdaten im manuellen Auskunftsverfahren

(1) Die Polizei kann zur Abwehr einer im einzelnen Falle bevorstehenden Gefahr von demjenigen, der geschäftsmäßig Telekommunikationsdienste erbringt oder daran mitwirkt (Diensteanbieter), Auskunft über die nach den §§ 95 und 111 des Telekommunikationsgesetzes vom 22. Juni 2004 (BGBl. I S. 1190), das zuletzt durch Artikel 1 des Gesetzes vom … (BGBl. I S. …)[2] geändert worden ist, erhobenen personenbezogenen Daten verlangen (§ 113 Absatz 1 Satz 1 des Telekommunikationsgesetzes). Bezieht sich das Auskunftsverlangen nach Satz 1 auf Daten, mittels derer der Zugriff auf Endgeräte oder auf Speichereinrichtungen, die in diesen Endgeräten oder hiervon räumlich getrennt eingesetzt werden, geschützt wird (§ 113 Absatz 1 Satz 2 des Telekommunikationsgesetzes), darf die Auskunft nur verlangt werden, wenn die gesetzlichen Voraussetzungen für die Nutzung der Daten vorliegen.

(2) Die Auskunft nach Absatz 1 darf auch anhand einer zu einem bestimmten Zeitpunkt zugewiesenen Internetprotokoll-Adresse verlangt werden (§ 113 Absatz 1 Satz 3 des Telekommunikationsgesetzes). In diesem Fall ist die betroffene Person über die Beauskunftung zu unterrichten. Die Unterrichtung erfolgt, soweit und sobald hierdurch der Zweck der Auskunft nicht vereitelt wird. Sie unterbleibt, wenn ihr überwiegende schutzwürdige Belange Dritter oder der betroffenen Person selbst entgegenstehen. Wird die Unterrichtung nach Satz 3 zurückgestellt oder nach Satz 4 von ihr abgesehen, sind die Gründe aktenkundig zu machen. Wurde die Unterrichtung zurückgestellt und ist sie fünf Jahre nach der Beauskunftung nicht möglich, ist der Landesbeauftragte für Datenschutz und Informationsfreiheit zu unterrichten.

(3) Aufgrund eines Auskunftsverlangens nach Absatz 1 oder Absatz 2 haben die Diensteanbieter die zur Auskunftserteilung erforderlichen Daten unverzüglich, vollständig und richtig zu übermitteln. Die in Anspruch genommenen Diensteanbieter werden entsprechend § 23 des Justizvergütungs- und -entschädigungsgesetzes vom 5. Mai 2004 (BGBl. I S. 718, 776), das zuletzt durch Artikel 13 des Gesetzes vom 5. Dezember 2012 (BGBl. I S. 2418) geändert worden ist, entschädigt.“

3. § 34a wird wie folgt geändert:

   a) In Absatz 2 Nummer 2 wird die Angabe „vom 22. Juni 2004 (BGBl. I S. 1190), das zuletzt durch Artikel 2 des Gesetzes vom 17. Februar 2010 (BGBl. I S. 78) geändert worden ist,“ gestrichen.

---

[2] Siehe Fußnote 1.

b) Absatz 6 wird wie folgt geändert:

aa) In Satz 1 werden die Wörter „hat jeder, der geschäftsmäßig Telekommunikationsdienstleistungen erbringt oder daran mitwirkt (Diensteanbieter),“ durch die Wörter „haben die Diensteanbieter“ ersetzt.

bb) In Satz 2 wird die Angabe „vom 5. Mai 2004 (BGBl. I S. 718, 776), das zuletzt durch Artikel 7 Absatz 3 des Gesetzes vom 30. Juli 2009 (BGBl. I S. 2449) geändert worden ist,“ gestrichen.

Artikel 3
Einschränkung von Grundrechten

Durch die Artikel 1 und 2 wird das Recht auf Wahrung des Fernmeldegeheimnisses (Artikel 10 Absatz 1 des Grundgesetzes) eingeschränkt.

Artikel 4
Inkrafttreten

Dieses Gesetz tritt am 1. Juli 2013 in Kraft.

Begründung:

I. Allgemeine Begründung

Zur Erfüllung der ihr im Rahmen der Gefahrenabwehr obliegenden Aufgaben kann die Polizei des Landes Mecklenburg-Vorpommern aufgrund der bestehenden allgemeinen Datenerhebungsvorschriften im Sicherheits- und Ordnungsgesetz von geschäftsmäßigen Anbietern von Telekommunikationsdiensten (Diensteanbieter) Datenauskünfte gemäß § 113 Absatz 1 des Telekommunikationsgesetzes (TKG) erhalten. Diese Möglichkeit steht auch der Verfassungsschutzbehörde zur Erfüllung ihrer Aufgaben aufgrund der im Landesverfassungsschutzgesetz enthaltenen allgemeinen Datenerhebungsbefugnisse zur Verfügung. Im Einzelnen konnten nach diesem sogenannten manuellen Auskunftsverfahren von den Diensteanbietern bisher Auskünfte über

- Daten nach § 95 TKG (sogenannte Daten zum Vertragsverhältnis, unter anderem Name und Anschrift des Teilnehmers),
- Daten nach § 111 TKG (sogenannte Kunden- oder Teilnehmerdaten, in der Regel umfangreicher als der Datenbestand nach § 95 TKG, zum Beispiel Rufnummer und andere Anschlusskennungen, Name, Anschrift, Geburtsdatum des Anschlussinhabers, Gerätenummern von Mobilfunkendgeräten etc.),
- Daten, mittels derer der Zugriff auf Endgeräte oder in diesen oder auch hiervon räumlich getrennt eingesetzten Speichereinrichtungen geschützt wird (Zugangssicherungscodes wie PIN und PUK) und
- Daten zur Identifizierung von Internet-Protokolladressen

verlangt werden.

Das Bundesverfassungsgericht hat am 24. Januar 2012 jedoch im Rahmen einer Verfassungsbeschwerde gegen mehrere Vorschriften im TKG unter anderem auch über die Verfassungsmäßigkeit der Regelungen zum manuellen Auskunftsverfahren in § 113 TKG entschieden (Az.: 1 BvR 1299/05). Es kommt in seiner Entscheidung zu dem Schluss, dass die Vorschrift so auszulegen ist, dass sie für Auskunftsverlangen in Bereichen, deren Regelung dem Landesrecht vorbehalten ist, spezifische Rechtsgrundlagen der Länder voraussetzt, die eine Auskunftsverpflichtung der Diensteanbieter eigenständig begründen. Demnach kann im TKG zwar die Befugnis für die Diensteanbieter geregelt werden, bestimmte Telekommunikationsdaten an die berechtigten Stellen zu übermitteln. Ergänzend bedarf es aber in den jeweiligen Fachgesetzen des Bundes und der Länder qualifizierter Vorschriften, die den berechtigten Stellen erlauben, diese Daten überhaupt von den Diensteanbietern zu verlangen (sogenanntes „Doppeltürenmodell“).

Zudem gelangte das Bundesverfassungsgericht zu der Auffassung, dass § 113 Absatz 1 Satz 1 TKG nicht als Rechtsgrundlage - wie bisher in der Praxis erfolgt - für eine Zuordnung von dynamischen Internetprotokoll-Adressen (IP-Adressen) zu ihren Anschlussinhabern herangezogen werden kann, da für diese Auskunft auf Verkehrsdaten zurückgegriffen werden muss und die Vorschrift hierzu erkennbar nicht ermächtigt.

Darüber hinaus stellte das Gericht fest, dass § 113 Absatz 1 Satz 2 TKG nicht mit dem Recht auf informationelle Selbstbestimmung vereinbar ist, da die Vorschrift die Auskunft über Zugangssicherungscodes (wie Passwörter, PIN oder PUK) nicht an die Bedingung knüpft, dass eine Auskunft über Sicherungscodes nur dann verlangt werden darf, wenn auch die rechtlichen Voraussetzungen für deren Nutzung erfüllt sind.

Aufgrund des sich aus dieser Entscheidung ergebenden, gesetzgeberischen Handlungsbedarfs - nämlich der Schaffung normenklarer Abrufregelungen im Bundes- und auch Landesfachrecht - hat das Bundesverfassungsgericht sich letztlich zur Schaffung einer Übergangsregelung veranlasst gesehen. Es hat die Anwendung des bestehenden § 113 TKG - teilweise unter zusätzlichen Maßgaben - längstens bis zum 30. Juni 2013 zugelassen. Hierzu führte das Gericht aus *„würden diese Anforderungen sofort wirksam, wären in zahlreichen Fällen […] Auskünfte zu Telekommunikationsnummern nicht mehr möglich. Auch könnten dynamische IP-Adressen bis zu einer Neuregelung nicht mehr identifiziert werden. Angesichts der Bedeutung solcher Auskünfte für die Aufklärung von Gefahren und Straftaten stehen die Nachteile eines solchen Ergebnisses in keinem Verhältnis zu der vorläufigen Hinnahme einer Praxis, die zwar formell den verfassungsrechtlichen Anforderungen nicht entspricht, aber im Wesentlichen rechtfertigungsfähig ist*" (siehe oben angegebene BVerfGE Absatz-Nr. 190).
Der Bundesgesetzgeber hat den Entwurf zur Änderung des Telekommunikationsgesetzes und zur Neuregelung der Bestandsdatenauskunft bereits vorgelegt (Bundestagsdrucksache 17/12034). Er sieht eine Neufassung des § 113 TKG vor. Auskünfte über die in § 113 Absatz 1 TKG aufgeführten Telekommunikationsdaten sollen durch die Diensteanbieter an die berechtigten Stellen zukünftig nur noch dann erteilt werden dürfen, wenn die jeweils berechtigte Stelle eine gesetzliche Bestimmung vorweisen kann, die ihr die Beauskunftung dieser Daten ausdrücklich erlaubt. Der Gesetzentwurf beschränkt sich auf die zur Umsetzung der nach der Bundesverfassungsgerichtsentscheidung notwendigen und durch den Bund möglichen Änderungen, um den Status quo aus Sicht des Bundes hinsichtlich der Gewährung von Bestandsdatenauskünften zu wahren. Er enthält jedoch keine Befugnisse zur Sicherung des Status quo beim Erlangen von Bestandsdatenauskünften durch die Landesbehörden. Die Schaffung dieser fällt in die Gesetzgebungszuständigkeit der Länder.

Damit die Möglichkeit der Abfrage von Bestandsdaten nach dem neugefassten § 113 TKG auch der Landespolizei und der Verfassungsschutzbehörde des Landes Mecklenburg-Vorpommern nach Auslaufen der vom Bundesverfassungsgericht gesetzten Übergangsfrist weiter zur Verfügung steht, besteht landesgesetzgeberischer Handlungsbedarf. Unter Beachtung der Vorgaben des Bundesverfassungsgerichts und der im neugefassten § 113 TKG gestellten Anforderungen an eine landesrechtliche Befugnisnorm bedarf es einer zwingenden Anpassung des Sicherheits- und Ordnungsgesetzes und des Landesverfassungsschutzgesetzes, damit die Landespolizei und die Verfassungsschutzbehörde nach Auslaufen der vom Bundesverfassungsgericht gesetzten Übergangsfrist weiterhin Auskünfte nach § 113 TKG erhalten können.

Ziel des vorliegenden Gesetzes ist es demnach, unter Beachtung der Vorgaben des Bundesverfassungsgerichts klare Bestimmungen zu treffen, unter welchen Voraussetzungen die Landespolizei und die Verfassungsschutzbehörde weiterhin Datenauskünfte nach § 113 TKG von den Diensteanbietern verlangen können. Hierzu werden das Sicherheits- und Ordnungsgesetz sowie das Landesverfassungsschutzgesetz entsprechend ergänzt. Dabei beschränken sich die mit diesem Gesetz jeweils vorgesehenen Ergänzungen auf die Sicherung des Status quo beim manuellen Beauskunftungsverfahren nach § 113 TKG für die Landespolizei und die Verfassungsschutzbehörde des Landes Mecklenburg-Vorpommern. Mit diesem Gesetz werden keine neuen Datenerhebungsbefugnisse für diese Behörden geschaffen. Vielmehr werden die derzeit auf Grundlage des Bundesrechts abgeforderten Datenauskünfte (bisheriger § 113 TKG) nun zukünftig unter Bezugnahme auf landesrechtliche Normen, die den verfassungsrechtlichen Vorgaben entsprechen, verlangt.

II. Zu den einzelnen Bestimmungen

Der Gesetzentwurf sieht aufgrund der erfolgten Neufassung der bundesrechtlichen Regelung in § 113 TKG Änderungen im Landesverfassungsschutzgesetz (Artikel 1) und im Sicherheits- und Ordnungsgesetz (Artikel 2) vor. Es werden unter Beachtung der bundesverfassungsrechtlichen Vorgaben klare, spezifische Bestimmungen in die Gesetze aufgenommen, unter welchen Voraussetzungen die Landespolizei und die Verfassungsschutzbehörde nunmehr Datenauskünfte nach dem neugefassten § 113 TKG von den Diensteanbietern verlangen können.

Zu Artikel 1

Mit dem Artikel 1 wird in das Landesverfassungsschutzgesetz unter Beachtung der Vorgaben des Bundesverfassungsgerichts eine Befugnis zur Erhebung von Telekommunikationsdaten im manuellen Auskunftsverfahren nach § 113 TKG eingefügt. Sie orientiert sich an der vom Bund geschaffenen Befugnis für das Bundesamt für Verfassungsschutz im Bundesverfassungsschutzgesetz und dient der Sicherung des Status quo bei der Beauskunftung von Daten im manuellen Auskunftsverfahren nach § 113 TKG für die Verfassungsschutzbehörde des Landes Mecklenburg-Vorpommern nach Wegfall der vom Bundesverfassungsgericht geschaffenen Übergangsregelung.

Zu Artikel 1 Nummer 1

Die Anpassung des Inhaltsverzeichnisses ist aufgrund der unter Nummer 2 vorgesehenen Gesetzesänderung - Einfügung eines § 24b in das Landesverfassungsschutzgesetz - erforderlich.

Zu Artikel 1 Nummer 2

Zu Absatz 1

In Absatz 1 wird die Berechtigung zur Abfrage von Bestandsdaten im manuellen Verfahren erteilt. Die Beauskunftung von Bestandsdaten ist nur im Einzelfall zulässig. Sie ist unerlässlich für die Arbeit der Verfassungsschutzbehörde, da in vielen Fällen nur anhand dieser Auskünfte mit vertretbarem Aufwand die Absender oder sonstigen Beteiligten an Kommunikationsvorgängen identifizierbar sind. In der Vergangenheit wurde die Befugnis auf § 7 Absatz 1 des Landesverfassungsschutzgesetzes in Verbindung mit § 113 Absatz 1 Satz 1 des Telekommunikationsgesetzes gestützt. Das Bundesverfassungsgericht hat festgestellt, dass eine explizite und qualifizierte Regelung in den jeweiligen Fachgesetzen erforderlich ist. Diese wird für die Verfassungsschutzbehörde nun im Landesverfassungsschutzgesetz geschaffen. Neue Befugnisse werden hierdurch nicht erteilt.

Zu Absatz 2

Die Bestandsdatenauskunft ist vielfach ausschließlich anhand einer vorhandenen dynamischen, also nur für kurze Zeit zugeteilten, IP-Adresse möglich. Damit die berechtigten Stellen solche Auskünfte zukünftig weiter erhalten können, bedarf es laut Bundesverfassungsgericht ausdrücklicher Regelungen im § 113 TKG und im Fachrecht des Bundes und der Länder.
Vor diesem Hintergrund hat einerseits der Bundesgesetzgeber im neugefassten § 113 Absatz 1 TKG nun ausdrücklich geregelt, dass die in eine Auskunft aufzunehmenden Daten auch anhand einer zu einem bestimmten Zeitpunkt zugewiesenen IP-Adresse bestimmt werden dürfen und hierzu auch eine automatisierte Auswertung von Verkehrsdaten erfolgen darf. Anderseits bedarf es aber nach dem „Doppeltürenmodell" auch einer normenklaren Befugnis im Landesverfassungsschutzgesetz, die der Verfassungsschutzbehörde das Einholen dieser Daten im manuellen Auskunftsverfahren erlaubt. Mit der Regelung in Absatz 2 wird eine solche nunmehr geschaffen.

Zu Absatz 3

Absatz 3 Satz 1 trägt dem Grundsatz der Transparenz Rechnung und führt eine Benachrichtigungspflicht gegenüber der von der Beauskunftung nach Absatz 2 betroffenen Person ein. Vor dem Hintergrund, dass die Datenbeauskunftung zur Zuordnung von dynamischen IP-Adressen im Gegensatz zur Beauskunftung von Daten, die nach den §§ 95 und 111 TKG erhoben wurden, mit einem Eingriff in Artikel 10 Absatz 1 GG einhergeht, wird durch die Benachrichtigungspflicht die Möglichkeit der Erlangung nachträglichen Rechtsschutzes eröffnet.

Die Regelung einer Benachrichtigung in Fällen einer Beauskunftung von Zugangssicherungscodes ist nicht erforderlich, da die Beauskunftung durch die Verfassungsschutzbehörde nur dann verlangt werden darf, wenn die gesetzlichen Voraussetzungen ihrer Nutzung gegeben sind.

Die Sätze 2 und 3 enthalten unter Berücksichtigung der Entscheidung des Bundesverfassungsgerichts vom 2. März 2010 - Az.: 1 BvR 256/08 - die Ausnahmen von der Benachrichtigungspflicht (siehe Absatz-Nummer 263). So ist zum einen in Satz 2 bestimmt, dass die Benachrichtigung der von der Datenbeauskunftung zur Zuordnung von dynamischen IP-Adressen betroffenen Person zurückzustellen ist, soweit und sobald eine Gefährdung des Zwecks der Auskunft und der Eintritt übergreifender Nachteile für das Wohl des Bundes oder eines Landes nicht ausgeschlossen werden kann. Satz 3 sieht vor, dass die Benachrichtigung ausnahmsweise unterbleiben darf, wenn ihr überwiegende schutzwürdige Belange Dritter oder der betroffenen Person selbst entgegenstehen. Hier ist also jeweils eine Abwägung im Einzelfall erforderlich.

Satz 4 enthält ebenfalls entsprechend der Entscheidung des Bundesverfassungsgerichts vom 2. März 2010 eine Dokumentationspflicht hinsichtlich der Gründe für ein Zurückstellen bzw. das Absehen von der Benachrichtigung (siehe auch hierzu Absatz-Nummer 263).

Zu Absatz 4

Mit dieser Regelung werden die Diensteanbieter ausdrücklich zur Auskunftserteilung verpflichtet.

Zu Absatz 5

In Absatz 5 wird die Verpflichtung zur Entschädigung der verpflichteten Unternehmen nach den einschlägigen Regelungen des Justizvergütungs- und -entschädigungsgesetzes festgeschrieben.

Zu Absatz 6

Eine Bestandsdatenauskunft anhand dynamischer IP-Adressen stellt nach Maßgabe des Bundesverfassungsgerichtes einen Eingriff in das Fernmeldegeheimnis nach Artikel 10 des Grundgesetzes dar. Für derartige Eingriffe gilt das Zitiergebot gemäß Artikel 19 Absatz 1 Satz 2 des Grundgesetzes. Diesem wird - zusätzlich zu Artikel 3 - mit dieser Vorschrift entsprochen.

Zu Artikel 2

Mit Artikel 2 wird in das Sicherheits- und Ordnungsgesetz ebenfalls unter Beachtung der Vorgaben des Bundesverfassungsgerichts eine Befugnis zur Beauskunftung von Telekommunikationsdaten im manuellen Verfahren nach dem neu gefassten § 113 TKG eingefügt.

Die Befugnis ist erforderlich, damit die Polizei weiterhin auch zur Gefahrenabwehr Bestandsdatenauskünfte von den Dienstanbietern erhalten kann. Beispiele für solche Datenauskünfte sind Suizidankündigungen sowie veröffentlichte Drohungen (zum Beispiel Ankündigungen eines Amoklaufs) im Internet, die ein unverzügliches Einschreiten zur Ermittlung der suizidgefährdeten beziehungsweise zur Ermittlung der für eine Gefahr verantwortlichen Person erforderlich machen. Zur Identifizierung der Betroffenen und damit der Abwehr von Gefahren für Leib oder Leben ist ein zeitnahes Erlangen von Bestandsdaten zum Beispiel im Zusammenhang mit IP-Adressen oder E-Mail-Accounts notwendig. Das Erfordernis derartiger Datenbeauskunftungen kann im Bereich der Gefahrenabwehr zum Beispiel auch bei Stalking im Anfangsstadium oder zur Ad-hoc-Abklärung bei Anrufen mit unklarer Intention gegeben sein.
Darüber hinaus werden mit Artikel 2 Folgeanpassungen vorgenommen.

Zu Artikel 2 Nummer 1

Die Anpassung des Inhaltsverzeichnisses ist aufgrund der unter Nummer 2 vorgesehenen Gesetzesänderung - Einfügung eines § 28a in das Sicherheits- und Ordnungsgesetz - erforderlich.

Zu Artikel 2 Nummer 2

Zur Erfüllung der ihr im Rahmen der Gefahrenabwehr obliegenden Aufgaben, kann die Polizei des Landes Mecklenburg-Vorpommern derzeit aufgrund der bestehenden, allgemeinen Datenerhebungsvorschriften im Sicherheits- und Ordnungsgesetz von den Diensteanbietern bestimmte Datenauskünfte gemäß § 113 Absatz 1 TKG erhalten. Diese Möglichkeit besteht mit Blick auf die vom Bundesverfassungsgericht festgelegte Übergangsfrist nur noch bis zum 30. Juni 2013. Wie bereits ausgeführt, hat das Bundesverfassungsgericht entschieden, dass spätestens ab diesem Zeitpunkt nach dem bereits erwähnten „Doppeltürenmodell" neben der im TKG zu regelnden Befugnis für die Diensteanbieter, bestimmte Telekommunikationsdaten an die berechtigten Stellen zu übermitteln, auch in den jeweiligen Fachgesetzen des Bundes und der Länder qualifizierte Vorschriften vorliegen müssen, die den berechtigten Stellen erlauben, diese Daten im Auskunftsverfahren zu verlangen. Andernfalls scheidet eine Auskunftserteilung nach § 113 TKG aus.

Unter Beachtung der Vorgaben des Bundesverfassungsgerichts hat der Bundesgesetzgeber deshalb § 113 TKG neugefasst und dort in Absatz 2 geregelt, dass Auskünfte über

- Daten nach § 95 TKG (sogenannte Daten zum Vertragsverhältnis, unter anderem Name und Anschrift des Teilnehmers),
- Daten nach § 111 TKG (sogenannte Kunden- oder Teilnehmerdaten, in der Regel umfangreicher als der Datenbestand nach § 95 TKG, zum Beispiel Rufnummer und andere Anschlusskennungen, Name, Anschrift, Geburtsdatum des Anschlussinhabers, Gerätenummern von Mobilfunkendgeräten etc.),
- Daten, mittels derer der Zugriff auf Endgeräte oder in diesen oder auch hiervon räumlich getrennt eingesetzten Speichereinrichtungen geschützt wird (Zugangssicherungscodes wie PIN und PUK) und
- Daten zur Identifizierung von Internet-Protokolladressen

durch die Provider an die berechtigten Stellen nur dann erteilt werden dürfen, wenn die jeweilige Stelle eine gesetzliche Bestimmung vorweisen kann, die ihr eine Beauskunftung dieser Daten ausdrücklich erlaubt (siehe Bundestagsdrucksache 17/12034).

Im Hinblick auf den Bereich der Verfolgung von Straftaten/Ordnungswidrigkeiten schafft der Bundesgesetzgeber bereits für die hier zuständigen Behörden - Staatsanwaltschaft, Polizei, Ordnungsbehörden - einen neuen § 100j Strafprozessordnung (StPO), der den Abruf der oben angegebenen Daten zulässt. Somit wird für den Bereich der Verfolgung von Straftaten und Ordnungswidrigkeiten zukünftig die geforderte, qualifizierte Rechtsgrundlage für die Datenbeauskunftung bestehen.

Für den Bereich der Gefahrenabwehr kann der Bund mit Blick auf seine Gesetzgebungszuständigkeit keine Regelungen treffen. Vielmehr fällt es in die Zuständigkeit der Landesgesetzgeber, entsprechende landesrechtliche Vorschriften zu schaffen, die es der Polizei im Land Mecklenburg-Vorpommern auch zukünftig erlauben, die oben angegebenen Daten im Auskunftsverfahren von den Diensteanbietern zu verlangen.

Dementsprechend wird ein § 28a in das Sicherheits- und Ordnungsgesetz eingefügt, der die Beauskunftung von Telekommunikationsdaten im manuellen Verfahren künftig im Bereich der Gefahrenabwehr ausdrücklich regeln soll. Die Regelung orientiert sich an den vom Bund geschaffenen fachrechtlichen Befugnissen für die Bundespolizei.

Zu Absatz 1

Satz 1 der vorgeschlagenen Regelung enthält die Befugnis für die Polizei, im manuellen Auskunftsverfahren nach § 113 TKG die nach den §§ 95 und 111 TKG gespeicherten Daten vom Diensteanbieter verlangen zu dürfen.
Das Bundesverfassungsgericht fordert das Vorliegen einer konkreten Gefahr als Voraussetzung für solche Auskünfte (siehe oben angegebene BVerfGE Absatz-Nummer 177). Demnach sieht der Gesetzentwurf vor, dass die Datenauskunft nur zur Abwehr einer im einzelnen Falle bevorstehenden Gefahr verlangt werden darf. Gemäß § 3 Absatz 3 Nummer 1 muss also eine Sachlage gegeben sein, bei der bei ungehindertem Ablauf des objektiv zu erwartenden Geschehens ein die öffentliche Sicherheit oder Ordnung schädigendes Ereignis im konkreten Einzelfall in absehbarer Zeit mit hinreichender Wahrscheinlichkeit eintreten wird. Diese Eingriffsschwelle ist nach den Ausführungen des Bundesverfassungsgerichts notwendig, aber auch ausreichend. So führt das Gericht in der oben genannten Entscheidung aus:
„Bezogen auf die Gefahrenabwehr, in die der Gesetzgeber die Gefahrenvorsorge gerade nicht einbezogen hat, ergibt sich bei verständiger Auslegung das Erfordernis einer ‘konkreten Gefahr‘ im Sinne der polizeilichen Generalklauseln als Voraussetzung für solche Auskünfte. Diese Schwelle ist freilich niedrig und umfasst auch den Gefahrenverdacht. Ebenso beschränkt sie Auskünfte nicht von vornherein auf Polizeipflichtige im Sinne des allgemeinen Polizei- und Ordnungsrechts. Sie ist damit jedoch nicht so entgrenzt, dass sie angesichts des gemäßigten Eingriffsgewichts unverhältnismäßig wäre. Insbesondere werden damit Auskünfte nicht als allgemeines Mittel für einen gesetzesmäßigen Verwaltungsvollzug ermöglicht, sondern setzen im Einzelfall einen sicherheitsrechtlich geprägten Charakter der betreffenden Aufgabe voraus. […] Insgesamt sind diese Schwellen zwar nicht hoch, aber verfassungsrechtlich noch hinnehmbar. Hierbei ist im Vergleich zu § 112 TKG zu berücksichtigen, dass ein manuelles Auskunftsverfahren für die abfragende Behörde einen gewissen Verfahrensaufwand mit sich bringt, der dazu beitragen dürfte, dass die Behörde die Auskunft nur bei hinreichendem Bedarf einholt“ (siehe oben angegebene BVerfGE Absatz-Nummer 177, 178).
Satz 2 legt ausdrücklich fest, dass die Befugnis nach Satz 1 auch für eine Auskunftserteilung über Daten, mittels derer der Zugriff auf Endgeräte oder auf Speichereinrichtungen, die in diesen Endgeräten oder hiervon räumlich getrennt eingesetzt werden, geschützt wird (unter anderem PIN und PUK), gilt. Entsprechend der Vorgabe des Bundesverfassungsgerichts wird hier aber zusätzlich gefordert, dass eine Auskunft über Sicherungscodes nur dann verlangt werden darf, wenn die gesetzlichen Voraussetzungen für die Nutzung dieser Codes vorliegen. So führte das Gericht in seiner oben angesprochenen Entscheidung aus: *„Die Frage, wann die Behörden von den Sicherungscodes Gebrauch machen und auf die durch sie gesicherten Daten und Telekommunikationsvorgänge Zugriff nehmen dürfen, bestimmt sich vielmehr nach eigenständigen Rechtsgrundlagen, wie § 113 Abs. 1 Satz 3 TKG für Eingriffe in das Telekommunikationsgeheimnis ausdrücklich klarstellt“* (siehe Absatz-Nummer 184).

Soll also eine Auskunft über Zugangssicherungscodes eingeholt werden, um eine Überwachung eines noch nicht abgeschlossenen Telekommunikationsvorgangs - und damit einen Eingriff in das Fernmeldegeheimnis - zu gefahrenabwehrrechtlichen Zwecken zu ermöglichen, ist § 34a des Sicherheits- und Ordnungsgesetzes (SOG M-V) zu berücksichtigen. Dies bedeutet, dass eine Auskunft nach § 113 TKG über Zugangssicherungscodes in diesen Fällen von der Polizei nur dann verlangt werden darf, wenn die in § 34a Absatz 1 enthaltenen, strengeren Voraussetzungen erfüllt sind. Insbesondere bedeutet dies auch, dass nach § 34a Absatz 4 eine richterliche Anordnung oder bei Gefahr im Verzug eine Anordnung des Behördenleiters beziehungsweise der Behördenleiterin oder einer von ihm oder ihr besonders beauftragten Person vorliegen muss.

Sollen demgegenüber mit den Zugangssicherungscodes zum Beispiel nach Sicherstellung eines Mobiltelefons gemäß § 61 SOG M-V auf diesem abgelegte Telekommunikationsdaten ausgelesen werden - also ein Zugriff auf Daten erfolgen, die bereits im Herrschaftsbereich des Betroffenen gespeichert sind -, gelten hierfür geringere Eingriffsschwellen. Denn für die beim Betroffenen gespeicherten Kommunikationsinhalte und -umstände bestehen nicht mehr dieselben spezifischen Risiken, wie sie sich aus der Nutzung einer Fernmeldeeinrichtung als Kommunikationsmedium ergeben. Der Schutzbereich des Fernmeldegeheimnisses endet in dem Moment, in dem eine Nachricht bei dem Empfänger angekommen und der Übertragungsweg beendet ist. Die im Herrschaftsbereich des Betroffenen gespeicherten personenbezogenen Daten (zum Beispiel selbst angelegtes Rufnummernverzeichnis/Adressliste auf dem Mobiltelefon oder einer PC-Festplatte) sind jedoch nicht ohne Schutz, sondern fallen unter den Schutz des Rechts auf informationelle Selbstbestimmung aus Artikel 2 Absatz 1 in Verbindung mit Artikel 1 Absatz 1 GG und gegebenenfalls unter den Schutz nach Artikel 13 Absatz 1 GG (siehe oben angegebene BVerfGE Absatz-Nummer 184 sowie auch BVerfGE 2 BvR 2099/04 vom 2. März 2006). Ist also zum Beispiel mit der Nutzung der Zugangssicherungscodes ein Auslesen der Daten, die auf einem sichergestellten Mobilfunktelefon abgelegt und damit im Herrschaftsbereich des Betroffenen gespeichert sind, mit dem Ziel deren Sicherstellung beabsichtigt, so kann eine Auskunft nach § 113 TKG in diesen Fällen von der Polizei verlangt werden, wenn die für die Sicherstellung geltenden Voraussetzungen (§ 61 ff. SOG M-V) vorliegen.

Welche gesetzlichen Voraussetzungen nach dem Sicherheits- und Ordnungsgesetz für eine Auskunft über die Zugangssicherungscodes nach § 113 TKG vorliegen müssen, bestimmt sich letztlich also danach, wofür die Codes konkret genutzt werden sollen. Es gilt, dass § 34a SOG M-V immer dann zu beachten ist, wenn mit den Sicherungscodes auf Daten zugegriffen werden soll, die dem Schutzbereich des Artikels 10 Absatz 1 GG unterfallen.

Zu Absatz 2

Die IP-Adresse ist eine Nummer, die die Adressierung von Computern und anderen technischen Geräten in einem Netzwerk, insbesondere im Internet, erlaubt; sie kann vereinfacht als „Telefonnummer“ des Computers beschrieben werden. Dabei wird zwischen statischen und dynamischen IP-Adressen unterschieden. Während eine statische IP-Adresse einem bestimmten Anschlussinhaber fest zugewiesen wird, wird im Fall der dynamischen Adressierung dem Anschlussinhaber bei jeder neuen Aufnahme der Netzwerkverbindung eine IP-Adresse neu zugewiesen.

Das Bundesverfassungsgericht stellte in seiner oben angegebenen Entscheidung fest, dass - im Gegensatz zur Zuordnung von statischen IP-Adressen - in der Zuordnung von dynamischen IP-Adressen ein Eingriff in Artikel 10 Absatz 1 GG liegt. Da § 113 TKG in der derzeit geltenden Fassung zu einem solchen Eingriff nicht ausdrücklich ermächtigt, darf die Vorschrift auch nicht zur Zuordnung dynamischer IP-Adressen angewendet werden (siehe oben angegebene BVerfGE Leitsätze 1 und 5). Das Gericht führt in der vorgenannten Entscheidung unter Absatz-Nummer 116 aus: *„Die Anwendbarkeit des Art. 10 Abs. 1 GG begründet sich hier […] daraus, dass die Telekommunikationsunternehmen für die Identifizierung einer dynamischen IP-Adresse in einem Zwischenschritt die entsprechenden Verbindungsdaten ihrer Kunden sichten müssen, also auf konkrete Telekommunikationsvorgänge zugreifen. Diese von den Diensteanbietern einzeln gespeicherten Telekommunikationsverbindungen fallen unter das Telekommunikationsgeheimnis, unabhängig davon, ob sie von den Diensteanbietern aufgrund gesetzlicher Verpflichtung vorrätig gehalten werden müssen (vgl. BVerfGE 125, 260 <312 f.>) oder von ihnen auf vertraglicher Grundlage gespeichert werden. Soweit der Gesetzgeber die Telekommunikationsunternehmen dazu verpflichtet, auf diese Daten zurückzugreifen und sie für die staatliche Aufgabenwahrnehmung auszuwerten, liegt darin ein Eingriff in Art. 10 Abs. 1 GG. Dies ist nicht nur dann der Fall, wenn die Diensteanbieter die Verbindungsdaten selbst herausgeben müssen, sondern auch dann, wenn sie sie als Vorfrage für eine Auskunft nutzen müssen“.*

Um also zukünftig eine Auskunft über eine zu einem bestimmten Zeitpunkt zugewiesenen IP-Adresse erhalten zu können, hat einerseits der Bundesgesetzgeber im neugefassten § 113 Absatz 1 TKG nun ausdrücklich geregelt, dass die in eine Auskunft aufzunehmenden Daten auch anhand einer zu einem bestimmten Zeitpunkt zugewiesenen IP-Adresse bestimmt werden dürfen und hierzu auch eine automatisierte Auswertung von Verkehrsdaten erfolgen darf. Anderseits bedarf es aber nach dem „Doppeltürenmodell“ auch einer normenklaren Befugnis im Gefahrenabwehrrecht des Landes Mecklenburg-Vorpommern, die der Polizei das Einholen dieser Daten im manuellen Auskunftsverfahren erlaubt.

Mit Satz 1 wird eine solche Befugnis in § 28a Absatz 2 aufgenommen. Unter den Voraussetzungen des Absatzes 1 - also der dort geregelten Eingriffsschwelle (Abwehr einer im einzelnen Falle bevorstehenden Gefahr) - darf eine Auskunft von den Diensteanbietern auch anhand einer zu einem bestimmten - also konkreten - Zeitpunkt zugewiesenen IP-Adresse verlangt werden.

Satz 2 trägt dem Grundsatz der Transparenz polizeilicher Maßnahmen Rechnung und führt eine Unterrichtungspflicht gegenüber der von der Beauskunftung nach Absatz 2 Satz 1 betroffenen Person ein. Vor dem Hintergrund, dass die Datenbeauskunftung zur Zuordnung von dynamischen IP-Adressen - wie bereits vorstehend ausgeführt - im Gegensatz zur Beauskunftung von Daten, die nach den §§ 95 und 111 TKG erhoben wurden, mit einem Eingriff in Artikel 10 Absatz 1 GG einhergeht, wird durch die Unterrichtungspflicht die Möglichkeit der Erlangung nachträglichen Rechtsschutzes eröffnet.

Die Regelung einer Unterrichtung in Fällen einer Beauskunftung von Zugangssicherungscodes ist nicht erforderlich, da die Beauskunftung durch die Polizei nur dann verlangt werden darf, wenn die gesetzlichen Voraussetzungen ihrer Nutzung gegeben sind. Insoweit bestimmt sich die Frage, wann die Polizei von den Sicherungscodes Gebrauch machen und auf die durch sie gesicherten Daten und Telekommunikationsvorgänge Zugriff nehmen darf, nach eigenen Rechtsgrundlagen (zum Beispiel § 34a SOG M-V, § 61 SOG M-V), die bereits schon Unterrichtungsregelungen enthalten (siehe § 34a Absatz 7 oder § 61 Absatz 2 SOG M-V). Diese Unterrichtungsregelungen greifen mithin immer, wenn die beauskunfteten Zugangssicherungscodes durch die Polizei genutzt werden.

Die Sätze 3 und 4 enthalten die Ausnahmen von der Unterrichtungspflicht, die das Bundesverfassungsgerichts selbst in seiner Entscheidung vom 2. März 2010 - Az.: 1 BvR 256/08 - formuliert hat (siehe Absatz-Nummer 263). So ist zum einen in Satz 3 bestimmt, dass die Unterrichtung der von der Datenbeauskunftung zur Zuordnung von dynamischen IP-Adressen betroffenen Person zurückzustellen ist, soweit und sobald hierdurch der Zweck der Auskunft vereitelt wird. Satz 4 sieht vor, dass die Unterrichtung ausnahmsweise unterbleiben darf, wenn ihr überwiegende schutzwürdige Belange Dritter oder der betroffenen Person selbst entgegenstehen. Hier ist also jeweils eine Abwägung im Einzelfall erforderlich.

Satz 5 enthält ebenfalls entsprechend der Entscheidung des Bundesverfassungsgerichts vom 2. März 2010 eine Dokumentationspflicht hinsichtlich der Gründe für ein Zurückstellen bzw. das Absehen von der Unterrichtung (siehe auch hierzu Absatz-Nummer 263).

In Satz 6 wird die bereits an anderen Stellen im SOG M-V aus datenschutzrechtlichen Gründen zu findende Regelungslage (siehe zum Beispiel § 34 Absatz 5 oder § 35 Absatz 3) übernommen, wonach im Falle einer Zurückstellung der Unterrichtung über einen Zeitraum von fünf Jahren nach Eingang der Datenauskunft, der Landesbeauftragte für Datenschutz und Informationsfreiheit zu unterrichten ist.

Zu Absatz 3

Satz 1 verpflichtet die Diensteanbieter ausdrücklich zur Auskunftserteilung.

Darüber hinaus wird mit Satz 2 - wie bereits bei Inanspruchnahme von Diensteanbietern bei Telekommunikationsüberwachungsmaßnahmen gemäß § 34a SOG M-V vorgesehen - geregelt, dass die Diensteanbieter für die Auskunftserteilung nach § 23 des Justizvergütungs- und -entschädigungsgesetzes zu entschädigen sind.

Dass durch die Maßnahmen, die durch § 28a getroffen werden können, bestimmte Grundrechte - insbesondere das Recht auf Wahrung des Fernmeldegeheimnisses (Artikel 10 Absatz 1 GG) - eingeschränkt werden, regelt bereits § 78 SOG M-V. Einer ausdrücklichen Regelung in § 28a SOG M-V bedarf es daher nicht. Im Übrigen wird auf Artikel 3 dieses Gesetzes hingewiesen.

Zu Artikel 2 Nummer 3

Bei den vorgesehenen Änderungen in § 34a SOG M-V handelt es sich um notwendige Gesetzesanpassungen aufgrund der in Artikel 2 Nummer 2 vorgesehenen Einfügung eines § 28a in das SOG M-V. Sie sind rein redaktioneller Natur.

So ist die in § 34a Absatz 2 Nummer 2 enthaltene Vollzitierung zum Telekommunikationsgesetz zukünftig bereits in § 28a Absatz 1 enthalten; sie kann daher in § 34a Absatz 2 Nummer 2 entfallen. Ebenfalls in § 28a Absatz 1 befindet sich die bisher in § 34a Absatz 6 Satz 1 enthaltene Erläuterung des Begriffes „Diensteanbieter"; sie ist daher in § 34a Absatz 6 Satz 1 entbehrlich. Da § 28a Absatz 3 zudem eine Vollzitierung zum Justizvergütung- und -entschädigungsgesetz enthält, bedarf es einer solchen in § 34a Absatz 6 Satz 2 nicht mehr.

Zu Artikel 3

Mit dem Artikel 3 wird dem verfassungsrechtlichen Zitiergebot gemäß Artikel 19 Absatz 1 Satz 2 des Grundgesetzes Rechnung getragen.

Zu Artikel 4

Artikel 4 regelt das Inkrafttreten. Da die Übergangsregelung des Bundesverfassungsgerichts am 30. Juni 2013 ausläuft und das „Gesetz zur Änderung des Telekommunikationsgesetzes und zur Neuregelung der Bestandsdatenauskunft" mit dem neu gefassten § 113 TKG am 1. Juli 2013[3] in Kraft tritt, müssen ab diesem Zeitpunkt auch die notwendigen Befugnisse in den Landesfachgesetzen für die Beauskunftung der in § 113 Absatz 1 TKG-Entwurf aufgeführten Telekommunikationsdaten zur Verfügung stehen. Denn mit dem Inkrafttreten des neu formulierten § 113 Absatz 2 TKG ist eine Auskunft durch die Diensteanbieter nur noch dann an die berechtigten Stellen zu erteilen, wenn eine gesetzliche Bestimmung durch diese Stellen vorgewiesen werden kann, die ihnen ausdrücklich eine Beauskunftung der in § 113 Absatz 1 TKG aufgeführten Daten erlaubt. Die Bestimmungen werden mit den Artikeln 1 und 2 dieses Gesetzentwurfs geschaffen.

[3] Derzeitiger Stand im Bundesgesetzgebungsverfahren (siehe Beschluss des Bundesrates vom 14.12.2012 zu Drucksache 664/12).